

Cryptographic Properties of the Welch–Gong Transformation Sequence Generators

Guang Gong, *Member, IEEE*, and Amr M. Youssef

Abstract—Welch–Gong (WG) transformation sequences are binary sequences of period $2^n - 1$ with two-level autocorrelation. These sequences were discovered by Golomb, Gong, and Gaal in 1998 and they verified the validity of their construction for $5 \leq n \leq 20$. Later, No, Chung, and Yun found another way to construct the WG sequences and verified their result for $5 \leq n \leq 23$. Dillon first proved this result for odd n in 1998, and, finally, Dobbertin and Dillon proved it for even n in 1999. In this paper, we investigate a two-faced property of the WG transformation sequences for application in stream ciphers and pseudorandom number generators. One is to present the randomness or unpredictability of the WG transformation sequences. The other is to exhibit the security properties of the WG transformations regarded as Boolean functions. In particular, we prove that the WG transformation sequences, in addition to the known two-level autocorrelation and three-level cross correlation with m -sequences, have the ideal 2-tuple distribution, and large linear span increasing exponentially with n . Moreover, it can be implemented efficiently. This is the first type of pseudorandom sequences with good correlation, statistic properties, large linear span, and efficient implementation. When WG transformations are regarded as Boolean functions, they have high nonlinearity. We derive a criterion for the Boolean representation of WG transformations to be r -resilient and show that they are at least 1-resilient under some basis of the finite field $\text{GF}(2^n)$. An algorithm to find such bases is given. The degree and linear span of WG transformations are presented as well.

Index Terms—Auto/cross correlation, Boolean function, linear span, nonlinearity, pseudorandom sequence (number) generator, r -resilient property, stream cipher.

I. INTRODUCTION

PSEUDORANDOM sequences have been widely used in communications and cryptology. Pseudorandom sequence generators are essential components in many cryptographic algorithms including stream-cipher algorithms, block-cipher algorithms, and pseudorandom number generators. The security of many stream-cipher and block-cipher systems is directly determined by the randomness or unpredictability of the employed pseudorandom sequence generators. In practical applications, a secure communication system that uses public key algorithms always employs a pseudorandom sequence generator as its session key or its private key generator. So, the security of the

system not only depends on the public key algorithms, but also relies on the security of such a pseudorandom sequence generator. In order to guarantee that the pseudorandom sequence generators have good randomness or unpredictability, we have the following criteria:

- long period;
- balance property (Golomb Postulate 1 [4]);
- run property (Golomb Postulate 2 [4]);
- n -tuple distribution;
- two-level autocorrelation (Golomb Postulate 3 [4]);
- low-level cross correlation;
- large linear span and smoothly increasing linear span profiles.

In the recent four years, there has been a celebrated event in the design of binary sequences with two-level autocorrelation. The researchers [3], [5], [10] [14] have found a number of new classes of binary sequences with two-level autocorrelation. In general, a pseudorandom sequence generator which generates sequences with two-level autocorrelation can be resistant to a correlation attack. However, it is not easy to design an efficient pseudorandom sequence generator which can generate sequences having both two-level autocorrelation and large linear span. Fortunately, one class of the new sequences with two-level autocorrelation, the so-called Welch–Gong (WG) transformation sequences, possesses all these three properties.

On the other hand, this type of sequences has period $2^n - 1$. Any binary sequence of period $2^n - 1$ is related to a function from the finite field $\text{GF}(2^n)$ to the finite field $\text{GF}(2)$. Thus, it is automatically related to a Boolean function in n variables. Therefore, there is a connection among binary sequences with period $2^n - 1$, polynomial functions from $\text{GF}(2^n)$ to $\text{GF}(2)$, and Boolean functions in n variables. Chang, Dai, and Gong [1] tried to use this connection. They applied m -sequences with three-level cross correlation to construct Boolean functions with maximal nonlinearity. In [7], Gong and Golomb applied tools in pseudorandom sequence design and analysis to analyze the S -boxes in the Data Encryption Standard (DES). When they considered the relationship between sequences and functions, they realized that monomials, which correspond to m -sequences, are not secure when used as component functions in block ciphers. This leads to the concept of linear span for polynomial functions, introduced in their work [7].

In this paper, we will investigate the WG transformation sequences as a two-faced subject. One is to present their randomness, i.e., autocorrelation, cross correlation with m -sequences, the balance property, and linear span when we consider them as

Manuscript received May 22, 2000; revised July 8, 2002. The work of G. Gong was supported by NSERC under Grants RGPIN 227700-00.

G. Gong is with the Electrical and Computer Engineering Department, University of Waterloo, Waterloo, ON N2L 3G1, Canada (e-mail: ggong@ece.uwaterloo.ca).

A. M. Youssef is with the Department of Electronics and Communications Engineering, Cairo University, Cairo, Egypt (e-mail: youssefa@yahoo.com).

Communicated by A. M. Klapper, Associate Editor for Sequences.

Digital Object Identifier 10.1109/TIT.2002.804043.

sequences. The other is to derive the nonlinearity, resilient property, linear span, and algebraic degree when they are regarded as Boolean functions.

This paper is organized as follows. In Section II, we give the definition of WG transformation sequences. In Section III, we present the randomness properties of the WG transformation sequences which include an irregular decimation property, statistic properties, cross correlation with m -sequences, the Hadamard transform, and the linear span. In Section IV, we derive a criterion for the resilient property (Note that since any WG transformation is balanced, the correlation immunity property becomes the resilient property.) and an algorithm for obtaining resilient bases. In Section V, we discuss linear span for the WG transformations regarded as Boolean functions and show their degrees. Section VI gives an example.

The reader is referred to [4] for the theory of shift-register sequences, [8] for the theory of finite fields, and [18] and [17] for the motivation and the original definitions of nonlinearity and the resilient property for Boolean functions.

We conclude this section by introducing the following notation which will be used throughout the paper.

- $\mathbb{F}_q = \text{GF}(q)$, a finite field with q elements; \mathbb{F}_q^* , the multiplication group of \mathbb{F}_q ; $\text{Tr}(x) = x + x^2 + \dots + x^{2^{n-1}}$, the trace function from \mathbb{F}_{2^n} to \mathbb{F}_2 .
- $\mathbb{F}_2^n = \{\mathbf{x} = (x_0, x_1, \dots, x_{n-1}) | x_i \in \mathbb{F}_2\}$, a vector space over \mathbb{F}_2 of dimension n .
- $\mathbf{a} = \{a_i\}$, $a_i \in \mathbb{F}_2$, a sequence over \mathbb{F}_2 , is called a *binary sequence*. If \mathbf{a} is a periodic sequence with period v , then we also denote $\mathbf{a} = (a_0, a_1, \dots, a_{v-1})$, an element in \mathbb{F}_2^v .
- $C_{\mathbf{a}}(\tau) = \sum_{i=0}^{v-1} (-1)^{a_i + a_{i+\tau}}$, $\tau = 0, 1, \dots$, the (periodic) autocorrelation function of \mathbf{a} . If

$$C_{\mathbf{a}}(\tau) = \begin{cases} v, & \text{if } \tau \equiv 0 \pmod{v} \\ -1, & \text{otherwise} \end{cases}$$

then we say that the sequence $\{a_i\}$ has ideal two-level autocorrelation function.

- $C_{\mathbf{a}, \mathbf{b}}(\tau) = \sum_{i=0}^{v-1} (-1)^{a_i + \tau + b_i}$, $\tau = 0, 1, \dots$, the (periodic) cross correlation of \mathbf{a} and $\mathbf{b} = (b_0, b_1, \dots, b_{v-1})$.
- $H(s) = |\{0 \leq i < 2^n - 1 | s_i = 1\}|$ if $s = \{s_i\}$ is a binary sequence with period $2^n - 1$ and $H(s) = |\{x \in \mathbb{F}_{2^n} | s(x) = 1\}|$ if $s = s(x)$ is a polynomial function from \mathbb{F}_{2^n} to \mathbb{F}_2 . In both cases, we call $H(s)$ the *Hamming weight* of s . For a positive integer $r = r_0 + r_1 2 + \dots + r_{n-1} 2^{n-1}$, $r_i \in \mathbb{F}_2$, $H(r) = |\{0 \leq i < n | r_i = 1\}|$ is also called the *Hamming weight* of the integer r .

II. DEFINITION OF WG TRANSFORMATION SEQUENCE GENERATORS

In this section, we will give the definition of the WG transformation sequence generators. From now on, we set $n \not\equiv 0 \pmod{3}$. Let $g(x) = x + x^{q_1} + x^{q_2} + x^{q_3} + x^{q_4}$, $x \in \mathbb{F}_{2^n}$, where the q_i 's are defined by

$$\begin{aligned} q_1 &= 2^k + 1 \\ q_2 &= 2^{2k-1} + 2^{k-1} + 1, \\ q_3 &= 2^{2k-1} - 2^{k-1} + 1 \end{aligned}$$

and

$$q_4 = 2^{2k-1} + 2^k - 1$$

for $n = 3k - 1$ and

$$\begin{aligned} q_1 &= 2^{k-1} + 1 \\ q_2 &= 2^{2k-2} + 2^{k-1} + 1 \\ q_3 &= 2^{2k-2} - 2^{k-1} + 1 \end{aligned}$$

and

$$q_4 = 2^{2k-1} - 2^{k-1} + 1$$

for $n = 3k - 2$. Then a function

$$f(x) = \text{Tr}(g(x+1) + 1), \quad x \in \mathbb{F}_{2^n} \quad (1)$$

is called the *WG transformation* of $\text{Tr}(g(x))$ in [10], or the *WG transformation* for short. Note that $f(x)$ is a function from \mathbb{F}_{2^n} to \mathbb{F}_2 . Let α be a primitive element of \mathbb{F}_{2^n} . Let $\mathbf{a} = \{a_i\}$ and $\mathbf{b} = \{b_i\}$ where

$$a_i = \text{Tr}(g(\alpha^i)), \quad i = 0, 1, \dots, \quad (2)$$

$$b_i = f(\alpha^i) = \text{Tr}(g(\alpha^i + 1) + 1), \quad i = 0, 1, \dots \quad (3)$$

Then \mathbf{b} is called a *WG transformation sequence* of \mathbf{a} , or a *WG sequence* for short.

Any function from \mathbb{F}_{2^n} to \mathbb{F}_2 is related to a Boolean function (we will discuss an exact conversion of these two representations in Section IV). From a WG transformation, we have two types of pseudorandom sequence generators. One is WG sequences themselves. The other is to apply WG transformations regarded as Boolean functions to operate on a set of linear feedback shift registers (LFSRs) for generating sequences. In other words, applying the WG transformations, regarded as Boolean functions, either as combining functions or filtering functions in combinatorial function generators, or filtering generators [15]. We refer to these two modes as *WG sequence generators*.

Remark 1: In fact, the transform given in (1) can be applied to any function from \mathbb{F}_{2^n} to \mathbb{F}_2 . But till now, we have not found any other type of $g(x)$ such that its WG transformation sequence has two-level autocorrelation. So, we restrict ourselves to this specific $g(x)$.

III. RANDOMNESS OF WG SEQUENCES

In this section, we will discuss the randomness properties of WG sequences, including their decimation, auto/cross correlation, statistic properties, and linear span.

A. Decimation Property

Lemma 1: Let α be a primitive element of \mathbb{F}_{2^n} and \mathbf{b} be the WG sequence of \mathbf{a} . Then the elements of \mathbf{b} can be obtained by operating an irregular decimation on \mathbf{a} as follows:

$$b_0 = a_0$$

and

$$b_i = \begin{cases} a_{\tau(i)}, & n \text{ even} \\ a_{\tau(i)} + 1, & n \text{ odd} \end{cases}$$

for $i > 0$, where $\tau(i)$ is determined by

$$\alpha^{\tau(i)} = \alpha^i + 1. \quad (4)$$

Proof: From the definition, $a_0 = \text{Tr}(g(1)) = n$ and $b_0 = \text{Tr}(g(0) + 1) = n$. Thus, $a_0 = b_0$. For $i > 0$, if n is even, we have

$$\begin{aligned} b_i &= \text{Tr}(g(\alpha^i + 1) + 1) = \text{Tr}(g(\alpha^i + 1)) + n \\ &= \text{Tr}(g(\alpha^i + 1)) = a_{t(i)}, \quad i = 0, 1, \dots \end{aligned}$$

Similarly, if n is odd, we have

$$\begin{aligned} b_i &= \text{Tr}(g(\alpha^i + 1) + 1) = \text{Tr}(g(\alpha^i + 1)) + n \\ &= \text{Tr}(g(\alpha^i + 1)) + 1 = a_{t(i)} + 1, \quad i = 0, 1, \dots \end{aligned}$$

Thus, the assertion is established. \square

Remark 2: Lemma 1 shows that the WG sequence \mathbf{b} can be obtained by an irregular decimation from \mathbf{a} where the decimation is determined by (4). Note that \mathbf{a} is a five-term sequence. So it can be generated by using five linear feedback shift registers and one AND gate. This property of the WG sequences allows them to have an efficient implementation for small n by operating decimation on \mathbf{a} together with a table lookup. Thus, we can use two methods to implement WG sequences. One is to use five LFSRs together with a table lookup (Lemma 1 method). The other is to use a finite-field configuration. The complexity of the implementation of WG sequences using the finite-field configuration depends only on the evaluation of four exponentiations. Especially, it requires only the evaluation of the exponents q_3 and q_4 where each of them has $k - 1$ consecutive 1's. We will discuss how to efficiently compute these two exponentiations in a separate paper. (Note that we can implement the trace function with no cost.)

B. Autocorrelation, Balance Property, and 2-Tuple Distribution

Proposition 1: Let \mathbf{b} be a WG sequence defined by (3). Then \mathbf{b} is a binary sequence of period $2^n - 1$ with (ideal) two-level autocorrelation.

This result was first discovered by Golomb, Gong, and Gaal in [10] and verified for $5 \leq n \leq 20$. Later, No *et al.* [14] found another way to construct the WG sequences and verified their result for $5 \leq n \leq 23$. Dillon [2] proved it for the odd n case, and finally, Dobbertin and Dillon [3] proved it for the even n case which completely established Proposition 1. (Note: \mathbf{a} is also a two-level autocorrelation sequence; see [10], [3].)

For a binary sequence $\mathbf{g} = (s_0, s_1, \dots, s_{2^n-2})$ of period $2^n - 1$ and $1 \leq t \leq n$, if each nonzero t -tuple $(c_1, c_2, \dots, c_t) \in \mathbb{F}_2^t$ occurs 2^{n-t} times and the zero t -tuple $(0, \dots, 0)$ occurs $2^{n-t} - 1$ times in every period of \mathbf{g} , then we say that the sequence has an *ideal t -tuple distribution*.

Any binary sequence with two-level autocorrelation satisfies the balance property and the 2-tuple distribution. This result can be easily obtained from their corresponding cyclic Hadamard difference sets. However, it is not trivial to see it from the point of view of sequences. So, we include a proof for this result for

completeness. Since a WG sequence has the two-level autocorrelation, it satisfies these two properties.

Proposition 2: Let $\mathbf{g} = (s_0, s_1, \dots, s_{2^n-2})$ be a binary sequence of period $2^n - 1$, and $H(\mathbf{g}) = w$, i.e., the Hamming weight of \mathbf{g} is w . For any $\tau \not\equiv 0 \pmod{2^n-1}$, let $H(\mathbf{g} + L^\tau(\mathbf{g})) = w'$ and

$$\Gamma = \{(s_k, s_{k+\tau}) | 0 \leq k < 2^n - 1\}.$$

Let

$$N_{ij} = |\{k | 0 \leq k < 2^n - 1, (s_k, s_{k+\tau}) = (i, j)\}|, \quad i, j \in \{0, 1\}.$$

Then
i)

$$N_{01} = N_{10} \quad (5)$$

$$N_{01} + N_{11} = w \quad (6)$$

$$N_{00} - N_{11} = 2^n - 1 - 2w \quad (7)$$

$$w' = \frac{2^n - 1 - C_{\mathbf{g}}(\tau)}{2}. \quad (8)$$

ii) If \mathbf{g} has the two-level autocorrelation, then

$$w = 2^{n-1}, \quad (9)$$

$$N_{01} = N_{10} = N_{11} = 2^{n-2} \quad \text{and} \quad N_{00} = 2^{n-2} - 1. \quad (10)$$

In other words, if \mathbf{g} is a two-level autocorrelation sequence, then \mathbf{g} is balanced with 2^{n-1} 1's in one period, and each nonzero 2-tuple $(i, j) \in \mathbb{F}_2^2$ occurs 2^{n-2} times in Γ and the $(0, 0)$ -tuple occurs $2^{n-2} - 1$ times in Γ .

Proof:

i) Note that

$$w' = N_{10} + N_{01}. \quad (11)$$

From the definitions of N_{ij} and the autocorrelation function, we have

$$N_{00} + N_{11} + N_{10} + N_{01} = 2^n - 1 \quad (12)$$

$$C_{\mathbf{g}}(\tau) = N_{00} + N_{11} - (N_{10} + N_{01}). \quad (13)$$

Together with (11), the result (8) is immediate. Note that \mathbf{g} and its phase shift $L^\tau \mathbf{g}$ have the same weight. By counting $(c, s_{k+\tau})$ and (s_k, c) where $c \in \mathbb{F}_2$ according to the weights of \mathbf{g} and $L^\tau(\mathbf{g})$, respectively, we have

$$N_{00} + N_{01} = 2^n - 1 - w \quad (14)$$

$$N_{10} + N_{11} = w \quad (15)$$

$$N_{00} + N_{10} = 2^n - 1 - w \quad (16)$$

$$N_{01} + N_{11} = w. \quad (17)$$

Thus, (17) gives the result (6). From (15) and (17), the result (5) is immediate. By substituting (5) into (14), then subtracting (6) from the resulting identity, we get (7). Thus, we established the result for the first part.

ii) Since $C_{\underline{g}}(\tau) = -1$ for $\tau \not\equiv 0 \pmod{2^n - 1}$, substituting this result into (8), we obtain $w' = 2^{n-1}$. Together with (5) and (11), we get

$$N_{10} = N_{10} = 2^{n-2}. \quad (18)$$

Note that

$$H(\underline{g} + L^T(\underline{g})) = H(\underline{g}) + H(L^T(\underline{g})) - 2N_{11} \implies w' = 2w - 2N_{11}.$$

Since $w' = 2^{n-1}$, the above identity yields $w - N_{11} = 2^{n-2}$. Combining this with (15) and (18), we get $w = 2^{n-1}$ which is (9). Substituting $w = 2^{n-2}$ and $N_{01} = 2^{n-2}$ into (15), we get $N_{11} = 2^{n-2}$. Substituting these values into (8), it follows that $N_{00} = 2^{n-2} - 1$. Combining with (18), the assertion (10) is established. \square

Corollary 1:

1) Any WG sequence is balanced, i.e., in every period $2^n - 1$, zeros occur $2^{n-1} - 1$ times and ones occur 2^{n-1} times.

2) Any WG sequence has the ideal 2-tuple distribution.

Proof: From Theorem 1, a WG sequence has the two-level autocorrelation. Applying Theorem 2, part ii), the result follows. \square

C. Hadamard Transform and Cross Correlation

Let $f(x)$ be a function from \mathbb{F}_{2^n} to \mathbb{F}_2 . Then the Hadamard transform of $f(x)$ is defined by

$$\hat{f}(\lambda) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{\text{Tr}(\lambda x) + f(x)}. \quad (19)$$

Let α be a primitive element in \mathbb{F}_{2^n} . If the two sequences $\underline{a} = \{a_i\}$ and $\underline{b} = \{b_i\}$ are given by $a_i = \text{Tr}(\alpha^i)$ and $b_i = f(\alpha^i)$, then the cross correlation of \underline{a} and \underline{b} and the Hadamard transform of $f(x)$ are related by the following identity:

$$C_{\underline{a}, \underline{b}}(\tau) = -1 + \hat{f}(\alpha^\tau). \quad (20)$$

Let $S_v(x) = \text{Tr}(x^v)$, $n = 2m + 1$ be odd and $v = 2^t + 1$ with $\text{gcd}(t, n) = 1$. Then the Hadamard transform of $S_{2^t+1}(x)$ is given by

$$\hat{S}_{2^t+1}(\lambda) = \begin{cases} 0, & \text{if } \text{Tr}(\lambda) = 0 \\ \pm 2^{m+1}, & \text{if } \text{Tr}(\lambda) = 1. \end{cases} \quad (21)$$

This has been established by Gold [6]. The method that Dillon used to prove that WG sequences are two-level autocorrelation sequences for n odd is to show that WG sequences have the same Hadamard transform as the m -sequences whose trace representation are given by $S_v(x) = \text{Tr}(x^v)$. Later, Dillon and Dobbertin established a similar result for all newly discovered two-level autocorrelation sequences. We state the Dillon's [2] milestone result in the following lemma.

Lemma 2 (Dillon [2]): For odd n , let $g(x)$ be defined as in Section II, and let $f(x)$ be the WG transform of $\text{Tr}(g(x))$, i.e., $f(x) = \text{Tr}(g(x+1))$. Then $\hat{f}(\lambda)$, the Hadamard transform of $f(x)$, is given by

$$\hat{f}(\lambda) = \hat{S}_{2^t+1}(\lambda^c)$$

where

$$c = d^{-1} \pmod{2^n - 1} \quad (22)$$

where

$$d = 2^{2t} - 2^t + 1, \quad \text{for } 3t = 1 \pmod{n}. \quad (23)$$

Combining with (21), the above result can be restated in the following two versions.

i) (**Function Version**) Let $n = 2m + 1$ be an odd integer, and let $f(x)$ be the WG transformation function. Then the Hadamard transform of $f(x)$ is given by

$$\hat{f}(\lambda) = \begin{cases} 0, & \text{if } \text{Tr}(\lambda^c) = 0 \\ \pm 2^{m+1}, & \text{if } \text{Tr}(\lambda^c) = 1. \end{cases}$$

ii) (**Sequence Version**) Let α be a primitive element of \mathbb{F}_{2^n} and $f(x)$ be a WG transformation function. Let $\underline{a} = \{a_i\}$ be an m -sequence whose elements are defined by

$$a_i = \text{Tr}(\alpha^i), \quad i = 0, 1, \dots$$

and $\underline{b} = \{b_i\}$ be the WG sequence whose elements are given by (3). Then, $C_{\underline{a}, \underline{b}}(\tau)$, the cross-correlation function between \underline{a} and \underline{b} , is determined by

$$C_{\underline{a}, \underline{b}}(\tau) = \begin{cases} -1, & \text{if } \text{Tr}(\alpha^{\tau^c}) = 0 \\ -1 \pm 2^{m+1}, & \text{if } \text{Tr}(\alpha^{\tau^c}) = 1. \end{cases}$$

In other words, the cross-correlation function between \underline{a} and \underline{b} are three-valued.

Note: The result ii) is derived together with (20).

D. Linear Span of WG Sequences

The linear span of a sequence is defined to be the *length* of the shortest linear feedback shift registers which can generate the sequence. Sequences with large linear span are resistant to attacks arising from employing the Berlekamp–Massey algorithm [12].

Proposition 3: Let \underline{b} be a WG sequence of period $2^n - 1$ and $\text{LS}(\underline{b})$ represent its linear span. Then

$$\text{LS}(\underline{b}) = n \left(2^{\lceil n/3 \rceil} - 3 \right).$$

We will give a proof for this result after we derive the linear span of the WG transformations in Section V. From Proposition 3, it is clear that the linear span of the WG sequences of period $2^n - 1$ increases exponentially with n .

Remark 3: WG sequences of period $2^n - 1$ are the first type of binary sequences of period $2^n - 1$ which have the balance property, ideal 2-tuple distribution, two-level autocorrelation, three-level cross correlation with m -sequences, and linear span increasing exponentially in n .

IV. RESILIENT PROPERTY OF WG TRANSFORMATIONS

In this section, we study the resilient property of the Boolean representations of WG transformations. Their nonlinearity can be directly obtained by combining the results of the function

version of Lemma 2 and the relationship between polynomial functions (from \mathbb{F}_{2^n} to \mathbb{F}_2) and Boolean functions in n variables. In the following, we will begin with developing a result on the conversion of a polynomial function (from \mathbb{F}_{2^n} to \mathbb{F}_2) to a Boolean function in n variables.

A. Isomorphism Between \mathbb{F}_{2^n} and \mathbb{F}_2^n

Since the finite field \mathbb{F}_{2^n} can be regarded as a vector space of n dimensions, then we have a linear space structure for \mathbb{F}_{2^n} . Let $\underline{\alpha} = \{\alpha_0, \alpha_1, \dots, \alpha_{n-1}\}$ be a basis of \mathbb{F}_{2^n} over \mathbb{F}_2 , then $\forall x \in \mathbb{F}_{2^n}$, we have

$$x = x_0\alpha_0 + x_1\alpha_1 + \dots + x_{n-1}\alpha_{n-1}, \quad x_i \in \mathbb{F}_2.$$

Let

$$\delta: x \mapsto \underline{x} = (x_0, x_1, \dots, x_{n-1}) \quad (24)$$

then $\delta(x)$ is an isomorphism between \mathbb{F}_{2^n} and \mathbb{F}_2^n when both of them are regarded as vector spaces.

A *Boolean function* is a function of n variables from \mathbb{F}_2^n to \mathbb{F}_2 , i.e., any Boolean function g can be represented as

$$g(x_0, \dots, x_{n-1}) = \sum a_{i_1, \dots, i_v} x_{i_1} \dots x_{i_v}, \quad a_{i_1, \dots, i_v} \in \mathbb{F}_2.$$

The *degree* of the Boolean function g is the largest v for which $a_{i_1, \dots, i_v} \neq 0$.

For any function $f(x)$ from \mathbb{F}_{2^n} to \mathbb{F}_2 , $f(x)$ can be represented by

$$f(x) = \sum_{i=1}^r \text{Tr}_1^{n_i}(\beta_i x^{t_i}), \quad \beta_i \in \mathbb{F}_{2^{n_i}} \quad (25)$$

where t_i is a coset leader of a cyclotomic coset modulo $2^{n_i} - 1$ and $n_i | n$ the size of the cyclotomic coset containing t_i (Note: This can be obtained by the discrete Fourier transform [13]. Also, it corresponds to the trace representation of a binary sequence with period $N | 2^n - 1$).

Lemma 3: With the above notation, $f(x)$ defines a Boolean function in the following way:

$$f(x) = f(x_0\alpha_0 + \dots + x_{n-1}\alpha_{n-1}) = f_{\underline{\alpha}}(x_0, x_1, \dots, x_{n-1})$$

where the Boolean function $f_{\underline{\alpha}}(x_0, x_1, \dots, x_{n-1})$ has degree r and r is the maximal values of $H(t_i)$'s, the Hamming weight of t_i .

Proof: From (25), it suffices to show that $\text{Tr}(\omega x^t)$ is a Boolean function in x_0, x_1, \dots, x_{n-1} of degree $H(t)$ when x is represented by $x = \sum_i x_i \alpha_i$. Let $\omega = \sum \omega_i \alpha_i$, $\omega_i \in \mathbb{F}_2$. Then

$$\omega x^t = \left(\sum_i \omega_i \alpha_i \right) \left(\sum_i x_i \alpha_i \right)^t = \sum_i D_i \alpha_i$$

where $D_i = D_i(x_0, x_1, \dots, x_{n-1}) \in \mathbb{F}_2$ is a Boolean function with degree $H(t)$. Therefore,

$$\text{Tr}(\omega x^t) = \text{Tr} \left(\sum_i D_i \alpha_i \right) = \sum_i \text{Tr}(D_i \alpha_i) = \sum_i D_i \text{Tr}(\alpha_i)$$

where $\text{Tr}(\alpha_i) \in \mathbb{F}_2$. Since $D_i(x_0, \dots, x_{n-1})$ is a Boolean function in variables x_0, x_1, \dots, x_{n-1} with degree $H(t)$, then $\text{Tr}(\omega x^t)$ defines a Boolean function of degree $H(t)$. Therefore, $f(x)$ defines a Boolean function of degree r where $r = \max_i \{H(t_i)\}$. \square

Note that f and $f_{\underline{\alpha}}$ in the above identity might not be same. We will write

$$f_{\underline{\alpha}}(x_0, x_1, \dots, x_{n-1}) = f(x_0, x_1, \dots, x_{n-1})$$

for short if it will not cause any confusion in the context.

Example 1: Let $n = 3$ and \mathbb{F}_{2^3} be defined by the irreducible polynomial $t(x) = x^3 + x + 1$. Let α be a root of $t(x)$. Then $\{1, \alpha, \alpha^2\}$ is a basis of \mathbb{F}_{2^3} over \mathbb{F}_2 . Let $f(x) = \text{Tr}(x^3)$. For any $x \in \mathbb{F}_{2^3}$, we write $x = x_0 + x_1\alpha + x_2\alpha^2$. Then

$$\begin{aligned} f(x) &= \text{Tr}(x^3) = \text{Tr}((x_0 + x_1\alpha + x_2\alpha^2)^3) \\ &= \text{Tr}(x_0 + x_1 + x_2 + x_1x_2) \\ &\quad + \text{Tr}((x_1 + x_0x_1 + x_0x_2)\alpha) + \text{Tr}((x_0x_1 + x_2)\alpha^2) \\ &= (x_0 + x_1 + x_2 + x_1x_2) + (x_1 + x_0x_1 + x_0x_2)\text{Tr}(\alpha) \\ &\quad + (x_0x_1 + x_2)\text{Tr}(\alpha^2) \\ &= x_0 + x_1 + x_2 + x_1x_2. \end{aligned}$$

The last identity is obtained by noting that $\text{Tr}(\alpha) = \text{Tr}(\alpha^2) = 0$.

From Lemma 3, for a given function $f(x)$ from \mathbb{F}_{2^n} to \mathbb{F}_2 , by representing $x = \sum_i x_i \alpha_i$, $x_i \in \mathbb{F}_2$ where $\{\alpha_0, \dots, \alpha_{n-1}\}$ is a basis of \mathbb{F}_{2^n} over \mathbb{F}_2 , we obtain a Boolean function, still written as $f(x_0, x_1, \dots, x_{n-1})$, by evaluating $f(x_0\alpha_0 + \dots + x_{n-1}\alpha_{n-1})$. We call $f(x_0, x_1, \dots, x_{n-1})$ a *Boolean representation or Boolean form* of $f(x)$ (with respect to the basis $\underline{\alpha}$).

When the defining polynomial of the finite field \mathbb{F}_{2^n} is fixed, a Boolean form of the function depends on the basis used for computation in \mathbb{F}_{2^n} regarded as a vector space. Since there are

$$B_n = \prod_{i=0}^{n-1} (2^n - 2^i)$$

different bases, there are B_n (not necessarily distinct) Boolean forms for a given function from \mathbb{F}_{2^n} to \mathbb{F}_2 . Conversely, for a given Boolean function in n variables, we can obtain its polynomial representation which is a function from \mathbb{F}_{2^n} to \mathbb{F}_2 by using the discrete Fourier transform or the Lagrange interpolation.

In the following, we will derive a conversion between the Walsh transform of Boolean functions and the Hadamard transform of their corresponding polynomial functions.

The *Walsh transform* of the Boolean function f is defined by

$$\hat{f}(\underline{w}) = \sum_{\underline{x} \in \mathbb{F}_2^n} (-1)^{\underline{w} \cdot \underline{x} + f(\underline{x})}. \quad (26)$$

Lemma 4: Let $f(\underline{x})$ be an arbitrary Boolean function and

$$a(\underline{x}) = \underline{w} \cdot \underline{x} = \sum_i w_i x_i$$

a linear Boolean function where $\underline{w} = (w_0, w_1, \dots, w_{n-1}) \in \mathbb{F}_2^n$. Let $f(x)$ and $a(x)$ be the polynomial representations of $f(\underline{x})$ and $a(\underline{x})$, respectively.

1) There exists some $\lambda \in \mathbb{F}_{2^n}$ such that

$$a(x) = \text{Tr}(\lambda x). \quad (27)$$

2) The Hadamard transform of $f(x)$ and the Walsh transform of $f(\underline{x})$ have the following relation:

$$\hat{f}(\underline{w}) = \hat{f}(\lambda), \quad \underline{w} \in \mathbb{F}_2^n, \lambda \in \mathbb{F}_{2^n} \quad (28)$$

where $\underline{w} \cdot \underline{x} = \text{Tr}(\lambda x)$.

Proof: In Lemma 3, we set $f(x) = \text{Tr}(\lambda x)$, then the first assertion follows immediately. We now consider the second assertion. Note that $f(x) = f(\underline{x})$. Thus, for $\underline{x} = (x_0, x_1, \dots, x_{n-1}) \in \mathbb{F}_2^n$, we have

$$\hat{f}(\underline{w}) = \sum_{\underline{x} \in \mathbb{F}_2^n} (-1)^{\underline{w} \cdot \underline{x} + f(\underline{x})} = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{\text{Tr}(\lambda x) + f(x)} = \hat{f}(\lambda)$$

where $\underline{w} \in \mathbb{F}_2^n$, $\lambda \in \mathbb{F}_{2^n}$, and $\underline{w} \cdot \underline{x} = \text{Tr}(\lambda x)$. So the second result is true. \square

The nonlinearity of $f(\underline{x})$, denoted by N_f , is defined as

$$N_f = \min_{a \in \mathcal{A}} d(f, a)$$

where $a(\underline{x})$ is an affine Boolean function in n variables, i.e.,

$$a(\underline{x}) = \sum_{i=0}^{n-1} w_i x_i + c, \quad w_i \in \mathbb{F}_2, c \in \mathbb{F}_2$$

\mathcal{A} is the set consisting of all affine Boolean functions in n variables and

$$d(f, a) = |\{\underline{x} \in \mathbb{F}_2^n | f(\underline{x}) \neq a(\underline{x})\}|.$$

Proposition 4: Let $n = 2m + 1$ and $f(x)$ be the WG transformation defined by (1). Let $f(\underline{x})$ be the Boolean form of $f(x)$. Then the nonlinearity of $f(\underline{x})$, denoted by N_f , is given by

$$N_f = 2^{n-1} - 2^m.$$

Proof: Note that

$$\hat{f}(\lambda) = 2^n - 2d(f, a)$$

where λ is determined by (27) in Lemma 4. The result follows directly from Dillon's fundamental result in the function version of Lemma 2. \square

B. Existence and Construction of r -Resilient WG Transformations

In this subsection, we will give a criterion for the Boolean representations of WG transformations to satisfy the resilient property and show that they are at least 1-resilient under some basis of $\mathbb{F}_{2^n}/\mathbb{F}_2$. An algorithm for finding such Boolean representations is also given.

Let $f(\underline{x})$, $\underline{x} \in \mathbb{F}_2^n$, be a Boolean function. For $r > 0$, $f(\underline{x})$ is said to be r -order correlation immune if

$$\hat{f}(\underline{w}) = 0, \quad \text{for all } \underline{w} \in \mathbb{F}_2^n: 1 \leq H(\underline{w}) \leq r. \quad (29)$$

This definition is due to the result obtained by Xiao and Massey [19], which is equivalent to Siegenthaler's original definition [17]. If $f(\underline{x})$ satisfies (29) and $f(\underline{x})$ is balanced, i.e., $H(f(\underline{x})) = 2^{n-1}$, then $f(\underline{x})$ is said to be r -resilient.

Let

$$D = \{x \in \mathbb{F}_{2^n}^* | \text{Tr}(x^c) = 0\} \quad (30)$$

where c is defined in Theorem 1. Then $|D| = 2^{n-1} - 1$. Recall that $\underline{\alpha} = (\alpha_0, \alpha_1, \dots, \alpha_{n-1})$ is the basis of $\mathbb{F}_{2^n}/\mathbb{F}_2$. Let

$$R_{\underline{\alpha}} = \{(\text{Tr}(\lambda \alpha_0), \dots, \text{Tr}(\lambda \alpha_{n-1})) \in \mathbb{F}_2^n | \lambda \in D\}. \quad (31)$$

Theorem 1: With the above notation. Let n be odd and let $f(\underline{x})$ be the Boolean form of the WG transformation $f(x)$ defined by (1). Then $f(\underline{x})$ is r -resilient if and only if all vectors in $W_r = \{\underline{w} | 1 \leq H(\underline{w}) \leq r\}$ appear in $R_{\underline{\alpha}}$, i.e., $W_r \subset R_{\underline{\alpha}}$.

Proof: Applying Lemma 4, we have

$$\hat{f}(\underline{w}) = \hat{f}(\lambda)$$

where

$$\underline{w} \cdot \underline{x} = \sum_{i=0}^{n-1} w_i x_i = \text{Tr}(\lambda x). \quad (32)$$

Notice that

$$\lambda x = \lambda \sum_i x_i \alpha_i \implies \text{Tr}(\lambda x) = \sum_{i=0}^{n-1} \text{Tr}(\lambda \alpha_i) x_i.$$

Combining with (32), we have

$$w_i = \text{Tr}(\lambda \alpha_i), \quad 0 \leq i < n. \quad (33)$$

According to the function version of Lemma 2, $\hat{f}(\lambda) = 0$ if and only if $\text{Tr}(\lambda^c) = 0$ where c is defined by (22). Together with the definition of the resilient property, we have the following reasoning process:

$$\begin{aligned} f \text{ is } r\text{-resilient} &\iff \hat{f}(\underline{w}) = 0 \text{ for all } \underline{w} \in W_r \\ &\iff \hat{f}(\lambda) = 0 \text{ for all } \lambda \text{ corresponding to} \\ &\quad \underline{w} \cdot \underline{x} = \text{Tr}(\lambda x), \underline{w} \in W_r \\ &\iff \text{for such } \lambda\text{'s, } \lambda \in D \text{ and} \\ &\quad (\text{Tr}(\lambda \alpha_0), \dots, \text{Tr}(\lambda \alpha_{n-1})) \in W_r \\ &\iff W_r \subset R_{\underline{\alpha}}. \quad \square \end{aligned}$$

Remark 4: Theorem 1 provides a method to find r -resilient WG transformations regarded as Boolean functions. Since the number of bases of \mathbb{F}_{2^n} is huge and $|R_{\underline{\alpha}}| = 2^{n-1} - 1$, it is possible to find Boolean forms of the WG transformations that have r -resilient property where r is in the range of $1 \leq r \leq n - \lceil n/3 \rceil$ (We will prove this inequality in the next section.)

In the following, we will prove that any WG transformation regarded as a Boolean function with 1-resilient property is always possible by a proper basis conversion.

Lemma 5: There are n linearly independent vectors in $R_{\underline{\alpha}}$, defined by (31).

Proof: Since the number of (distinct) vectors in $R_{\underline{\alpha}} \cup \{0\}$ is 2^{n-1} , the number of linearly independent vectors in $R_{\underline{\alpha}} \cup \{0\}$

is $\geq n-1$ with equality if and only if $R_{\underline{\alpha}} \cup \{0\}$ is a linear space. Now we will prove that $R_{\underline{\alpha}} \cup \{0\}$ is not a linear space. Assume that $R_{\underline{\alpha}} \cup \{0\}$ is a linear space of dimension $n-1$ and let

$$\sigma(\lambda) = (\text{Tr}(\lambda\alpha_0), \text{Tr}(\lambda\alpha_1), \dots, \text{Tr}(\lambda\alpha_{n-1})).$$

Thus, $\forall \lambda_1, \lambda_2 \in D$, we have $\sigma(\lambda_1)$ and $\sigma(\lambda_2) \in R$. Since R is a linear space, $\sigma(\lambda_1) + \sigma(\lambda_2) \in R$. Note that

$$\begin{aligned} \sigma(\lambda_1) + \sigma(\lambda_2) &= (\text{Tr}(\lambda_1\alpha_0) + \text{Tr}(\lambda_2\alpha_0), \text{Tr}(\lambda_1\alpha_1) + \text{Tr}(\lambda_2\alpha_1), \dots, \\ &\quad \text{Tr}(\lambda_1\alpha_{n-1}) + \text{Tr}(\lambda_2\alpha_{n-1})) \\ &= (\text{Tr}((\lambda_1 + \lambda_2)\alpha_0), \text{Tr}((\lambda_1 + \lambda_2)\alpha_1), \dots, \\ &\quad \text{Tr}((\lambda_1 + \lambda_2)\alpha_{n-1})) \in R. \end{aligned}$$

Hence $\lambda_1 + \lambda_2 \in D$. Therefore, $D \cup \{0\}$ is a linear space of dimension $n-1$. For any $x \in D$ and $\lambda \in D$, we have $\lambda+x \in D$. So, $\text{Tr}((\lambda+x)^c) = 0$ if $x \in D$ and $\text{Tr}((\lambda+x)^c) = 1$ if $x \notin D$. In other words, we have

$$\text{Tr}((\lambda+x)^c) = \begin{cases} 0, & \text{if } \text{Tr}(x^c) = 0 \\ 1, & \text{if } \text{Tr}(x^c) = 1. \end{cases}$$

Thus, $\text{Tr}((\lambda+x)^c) = \text{Tr}(x^c)$ which is a contradiction since $H(c) > 1$. \square

Theorem 2: Let $f(x)$ be a WG transformation, then there exists some basis of \mathbb{F}_{2^n} such that the Boolean representation of $f(x)$ under this basis is at least 1-resilient.

Proof: According to Lemma 5, we can assume that $\{\lambda_0, \dots, \lambda_{n-1}\}$ is a subset of $R_{\underline{\alpha}}$ which is linearly independent over \mathbb{F}_2 . We represent the elements of this basis by their vector forms under the basis $\underline{\alpha} = \{\alpha_0, \dots, \alpha_{n-1}\}$, i.e.,

$$\lambda_i = \sum_{k=0}^{n-1} \lambda_{i,k} \alpha_k, \quad \lambda_{i,k} \in \mathbb{F}_2.$$

From this, we form a matrix A whose i th row vector is $\underline{\lambda}_i = (\lambda_{i,0}, \dots, \lambda_{i,n-1})$, i.e.,

$$A = \begin{pmatrix} \underline{\lambda}_0 \\ \vdots \\ \underline{\lambda}_{n-1} \end{pmatrix}.$$

We form a new basis of $\mathbb{F}_{2^n}/\mathbb{F}_2$, say $\underline{\beta} = \{\beta_0, \beta_1, \dots, \beta_{n-1}\}$ which is given by

$$(\beta_0, \beta_1, \dots, \beta_{n-1}) = (\alpha_0, \alpha_1, \dots, \alpha_{n-1})A^{-1}.$$

Under this construction, we have

$$(\text{Tr}(\lambda\beta_0), \dots, \text{Tr}(\lambda\beta_{n-1})) = (\text{Tr}(\lambda\alpha_0), \dots, \text{Tr}(\lambda\alpha_{n-1}))A^{-1}.$$

Hence, $R_{\underline{\beta}}$ is given by

$$R_{\underline{\beta}} = \{(\text{Tr}(\lambda\alpha_0), \dots, \text{Tr}(\lambda\alpha_{n-1}))A^{-1} | \lambda \in D\}.$$

Therefore, the row vectors of $A^{-1}A = I_n$, the identity matrix, belong to $R_{\underline{\beta}}$. From Theorem 1, $f_{\underline{\beta}}(x_0, \dots, x_{n-1})$, the

Boolean representation of $f(x)$ under the basis $\underline{\beta}$, is a 1-resilient function. \square

From the proof of Lemma 5, the elements of a subset in $R_{\underline{\alpha}}$ are linearly independent over \mathbb{F}_2 if and only if the elements of the corresponding subset of D are linearly independent over \mathbb{F}_2 . Using this result and combining with the proof of Theorem 2, we have the following procedure to find a basis of \mathbb{F}_{2^n} over \mathbb{F}_2 such that a Boolean representation of the WG transformation under this basis is at least 1-resilience property. We call such a basis a *resilient basis*.

Algorithm 1. Finding Resilient Bases

Input: n , $0 < t < n$ such that $3t \equiv 1 \pmod{n}$, and $h(x)$, a primitive polynomial over \mathbb{F}_2 of degree n .

Output: $\underline{\beta} = \{\beta_0, \dots, \beta_{n-1}\}$, a resilient basis of $\mathbb{F}_{2^n}/\mathbb{F}_2$.

Procedure-RB($n, t, h(x)$):

Step 1. Generating the finite field \mathbb{F}_{2^n} defined by $h(x)$. Let α be a root of $h(x)$ and use the polynomial basis $\{1, \alpha, \dots, \alpha^{n-1}\}$ as a basis of $\mathbb{F}_{2^n}/\mathbb{F}_2$.

Step 2. Find n independent elements in D , defined by (30), i.e., $D = \{x \in \mathbb{F}_{2^n}^* | \text{Tr}(x^c) = 0\}$, say $\{\lambda_0, \dots, \lambda_{n-1}\}$.

Step 3. For $i = 0, 1, \dots, n-1$, compute

$$\sigma(\lambda_i) = (\text{Tr}(\lambda_i), \text{Tr}(\lambda_i\alpha), \dots, \text{Tr}(\lambda_i\alpha^{n-1})).$$

Form the matrix A where the i th row vector of A is $\sigma(\lambda_i)$, $i = 0, 1, \dots, n-1$.

Step 4. Find the inverse of A . Set

$$(\beta_0, \beta_1, \dots, \beta_{n-1}) = (1, \alpha, \dots, \alpha^{n-1})A^{-1}.$$

Return $\underline{\beta} = \{\beta_0, \dots, \beta_{n-1}\}$.

An example for applying this algorithm is given in Section VI.

V. LINEAR SPAN AND DEGREE OF WG TRANSFORMATIONS

The *linear span* of $f(x)$, introduced by Gong and Golomb in [7], is defined as the number of nonzero coefficients in $f(x) = \sum_i c_i x^i$. We denote it as $\text{LS}(f(x))$ or simply $\text{LS}(f)$ if the context is clear, i.e., $\text{LS}(f) = |I|$.

Remark 5: The linear span of a polynomial function from \mathbb{F}_{2^n} to \mathbb{F}_2 is equal to the linear span of the sequence that corresponds to the function.

Let $f(\underline{x})$ be a Boolean function, we will define the linear span of the Boolean function $f(\underline{x})$ in terms of its polynomial representations. Let

$$\Pi = \{\text{all bases of } \mathbb{F}_{2^n} \text{ over } \mathbb{F}_2\}.$$

For $\underline{\alpha} = \{\alpha_0, \dots, \alpha_{n-1}\} \in \Pi$, let $f_{\underline{\alpha}}(x)$ denote the polynomial representation of $f(\underline{x})$ with respect to the basis $\underline{\alpha}$. We define a *linear span* of $f(\underline{x})$, denoted by $\text{LS}(f(\underline{x}))$, as

$$\text{LS}(f(\underline{x})) = \min_{\underline{\alpha} \in \Pi} \text{LS}(f_{\underline{\alpha}}(x)).$$

Note that for a given polynomial function $f(x)$, the linear span of any Boolean representation of $f(x)$ is equal to the linear span of $f(x)$ itself. We will write this observation as a lemma for later reference.

Lemma 6: Let $f(x)$ be a polynomial function of \mathbb{F}_{2^n} to \mathbb{F}_2 and let $f_{\underline{\alpha}}(\underline{x})$ be its Boolean representation under the basis $\underline{\alpha}$. Then

$$\text{LS}(f_{\underline{\alpha}}(\underline{x})) = \text{LS}(f(x))$$

for all $\underline{\alpha} \in \Pi$.

As Youssef and Gong pointed it out in their recent work [20], the polynomial representation of a complicated Boolean function might be just a monomial function (here monomial means that it has only one trace term in (25) which is different from the concept of the ordinary monomial which only has exactly one term). A cryptographic Boolean function must have a large linear span so that it can be resistant to the interpolation attack. In the following, we will show that the linear span of the Boolean forms of the WG transformations increases exponentially with n .

The following result is extracted from [10].

Fact 1: Let $f(x) = \text{Tr}(g(x + 1) + 1)$ be the WG transformation defined by (1), then

$$f(x) = \sum_{i \in I} \text{Tr}(x^i) \tag{34}$$

where $I = I_1 \cup I_2$ for $n = 3k - 1$, where

$$I_1 = \{2^{2k-1} + 2^{k-1} + 2 + i \mid 0 \leq i \leq 2^{k-1} - 3\} \tag{35}$$

$$I_2 = \{2^{2k} + 3 + 2i \mid 0 \leq i \leq 2^{k-1} - 2\} \tag{36}$$

and where $I = \{1\} \cup I_3 \cup I_4$ for $n = 3k - 2$, where

$$I_3 = \{2^{k-1} + 2 + i \mid 0 \leq i \leq 2^{k-1} - 3\} \tag{37}$$

$$I_4 = \{2^{2k-1} + 2^{k-1} + 2 + i \mid 0 \leq i \leq 2^{k-1} - 3\}. \tag{38}$$

Moreover, in each case, all the elements in I belong to distinct cyclotomic cosets modulo $2^n - 1$.

Note that the trace functions that appear in (34) depend on the coset size of i in I .

Theorem 3: Let $f(x)$ be the WG transformation defined by (1), then $\text{LS}(f(x))$, the linear span of f , is given by

$$\text{LS}(f(x)) = n \left(2^{\lceil n/3 \rceil} - 3 \right).$$

Proof: According to Fact 1, all numbers in I belong to different cyclotomic cosets modulo $2^n - 1$ and $|I| = 2^k - 3$. So we only need to show that any coset containing a number in I has full size n . Here we only give a proof for $n = 3k - 1$ and $s \in I_1$, since proofs for the other cases are similar. Note that for $s \in I_1$, the binary representation of s has the following pattern:

$$\begin{array}{cccccccccccc} 0 & 1 & \cdots & k-1 & k & \cdots & 2k-2 & 2k-1 & 2k & \cdots & n-1 \\ x & x & \cdots & x & 0 & \cdots & 0 & 1 & 0 & \cdots & 0 \end{array} \tag{39}$$

where the first row denotes the index and the second row denotes the binary representation. In the above representation, x can take any value from $\{0, 1\}$. Let C_s be a coset containing s , then

$$C_s = \{s, s2, \dots, s2^{n_s-1}\}$$

where n_s is the smallest integer satisfying $s2^{n_s} \equiv s \pmod{2^n-1}$. According to (39), $n_s = n$, i.e., C_s has full size n . Thus, for each $s \in I$, the trace function in Fact 1 is the trace function

from \mathbb{F}_{2^n} to \mathbb{F}_2 . Therefore, $\text{LS}(\text{Tr}(x^i)) = n$ for each $i \in I$ which proves the theorem. \square

Proof of Proposition 3 in Section III: Since the linear span of a WG sequence \underline{b} is equal to the linear span of the corresponding WG transformation f , we have $\text{LS}(\underline{b}) = \text{LS}(f)$. Applying Theorem 3, the result follows.

Theorem 4: Let $f(x)$ be the WG transformation defined by (1). Then the linear span of any Boolean form of $f(x)$ is equal to the linear span of $f(x)$, i.e.,

$$\text{LS}(f(\underline{x})) = n \left(2^{\lceil n/3 \rceil} - 3 \right).$$

Proof: The result follows from Lemma 6 and Theorem 3. \square

Theorem 5: Let $f(x)$ be the WG transformation defined by (1) and $f(\underline{x})$ be its Boolean form. Then $\text{deg}(f(\underline{x}))$, the degree of $f(\underline{x})$, is given by

$$\text{deg}(f(\underline{x})) = \lceil n/3 \rceil + 1.$$

Proof: From Lemma 3, the degree of $f(\underline{x})$ is determined by the largest Hamming weight among the numbers in the set I in Fact 1.

Case 1. $n = 3k - 1$: In this case, I is defined by (35) and (36). Considering $i \in I_1$

$$\begin{aligned} i &= 2^{2k-1} + 2^{k-1} + 2 + 2^{k-1} - 3 \\ &= 2^{2k-1} + 2^k - 1 \implies H(i) = k + 1 \end{aligned}$$

which is the number in I_1 that has the largest Hamming weight among all the numbers in I_1 . For I_2 , the number in I_2 which has the largest Hamming weight is

$$i = 2^{2k} + 3 + 2(2^{k-1} - 2) = 2^{2k} + 2^k - 1 \implies H(i) = k + 1.$$

Therefore, $\text{deg}(f(\underline{x})) = k + 1$.

Case 2. $n = 3k - 2$: Similarly, we have

$$i = 2^{k-1} + 2 + 2^{k-1} - 3 = 2^k - 1 \in I_3 \implies H(i) = k$$

and

$$\begin{aligned} i &= 2^{2k-1} + 2^{k-1} + 2 + 2^{k-1} - 3 \\ &= 2^{2k-1} + 2^k - 1 \in I_4 \implies H(i) = k + 1. \end{aligned}$$

So, $i = 2^{2k-1} + 2^k - 1 \in I$ has the maximal Hamming weight among the all numbers in I . Therefore, $\text{deg}(f(\underline{x})) = k + 1$. \square

Corollary 2: For a given WG transformation regarded as a Boolean function in n variables, r , the order of the resilient property of the function is bounded by the following inequality:

$$r \leq n - \lceil n/3 \rceil.$$

Proof: Let d be the degree of the function. According to the Siegenthaler inequality [17] r , the order of the resilient property of the function d , the degree of the function, and n , the number of the variables have the following relation:

$$r + d \leq n - 1.$$

Applying Theorem 5, we have $d = \lceil n/3 \rceil + 1$. Therefore,

$$r \leq n - 1 - (\lceil n/3 \rceil + 1) = n - \lceil n/3 \rceil.$$

TABLE I
PROFILES OF WG TRANSFORMATIONS

WG Sequences Profile	WG Sequence	WG Trans. as boolean Func.	WG Trans. boolean Profile
$2^n - 1$	Period	\leftrightarrow boolean	n variables
Yes	Balance property	\leftrightarrow Balance property	Yes
Yes	2-tuple distribution	NC	
2-level	Auto correlation	NC	
$\{-1, -1 \pm 2^{\frac{n-1}{2}}\}$, n odd optimal w.r.t. the Welch bound,	cross correlation with m -sequences	\leftrightarrow Nonlinearity	$2^{n-1} - 2^{\frac{n-1}{2}}$, n odd
$0, \pm 2^{(n+1)/2}$, n odd	Hadamard transform spectrum		$0, \pm 2^{(n+1)/2}$, n odd
$n(2^{\lfloor n/3 \rfloor} - 3)$ increases exponentially in n	Linear span	\Leftrightarrow Linear span	$n(2^{\lfloor n/3 \rfloor} - 3)$ increases exponentially in n
	NC	Degree	$\lfloor n/3 \rfloor + 1$
	NC	r -resilient	possible $r : 1 \leq r \leq n - \lfloor n/3 \rfloor$, n odd
Pseudo-random sequence generators	Applications		combining functions or filtering functions operating on a set of LFSRs

Or equivalently

$$r \leq \begin{cases} 2k - 2, & \text{for } n = 3k - 1 \\ 2k - 3, & \text{for } n = 3k - 2. \end{cases} \quad \square$$

VI. AN EXAMPLE

In this section, we will give an example to illustrate the randomness properties of WG transformations regarded as both WG sequences and Boolean functions, which we obtained in the previous sections. Let $n = 7$, then $k = 3$, and

$$q_1 = 5, \quad q_2 = 21, \quad q_3 = 13, \quad \text{and} \quad q_4 = 29.$$

So

$$g(x) = x + x^5 + x^{21} + x^{13} + x^{29}$$

and we have the WG transformation $f(x)$ given by

$$f(x) = \text{Tr}(g(x+1)+1) = \text{Tr}(x + x^3 + x^7 + x^{19} + x^{29}).$$

Let \mathbb{F}_{2^7} be defined by a primitive polynomial $h(x) = x^7 + x + 1$. Let α be a root of $h(x)$. Then α is a primitive element of \mathbb{F}_{2^7} .

a) *Sequence Aspects of the WG Transformation:* We obtain the elements in the first period of a WG sequence $\mathbf{b} = \{b_i\}$ as follows:

$$\begin{aligned} \mathbf{b} = & 1000000101000011011100 \\ & 0101001011001010100001 \\ & 0110001001011101101100 \\ & 0110011101100100000110 \\ & 0011110101011101001001 \\ & 11111100111101111 \end{aligned}$$

where $b_i = f(\alpha^i)$, $i = 0, 1, \dots$

The WG sequence \mathbf{b} has the following profiles:

- 1) balance property;
- 2) ideal 2-tuple distribution;
- 3) two-level autocorrelation;

- 4) three-valued cross correlation with an m -sequence $\{a_i\}$, $a_i = \text{Tr}(\alpha^i)$, $i = 0, 1, \dots$, belongs to the set $\{-1, 15, -17\}$;
- 5) the Hadamard transform spectrum belonging to the set $\{0, \pm 16\}$;
- 6) linear span 35.

b) *Boolean Function Aspects of the WG Transformation:* Using the polynomial basis

$$\underline{\alpha} = (1, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6)$$

where $\alpha^7 + \alpha + 1 = 0$, the algebraic normal form (obtained using the algorithm in [16]) of the Boolean function that corresponds to $f(x)$ under the basis $\underline{\alpha}$ is given by

$$\begin{aligned} & x_0 + x_1x_3 + x_2x_3 + x_0x_5 + x_3x_5 + x_1x_6 + x_2x_6 \\ & + x_4x_6 + x_0x_1x_3 + x_0x_2x_3 + x_1x_2x_3 + x_0x_3x_4 \\ & + x_2x_3x_4 + x_0x_1x_5 + x_0x_2x_5 + x_1x_2x_5 + x_1x_3x_5 \\ & + x_1x_4x_5 + x_2x_4x_5 + x_0x_2x_6 + x_0x_3x_6 + x_0x_4x_6 \\ & + x_2x_4x_6 + x_0x_5x_6 + x_1x_5x_6 + x_2x_3x_4x_5 + x_1x_3x_4x_6 \\ & + x_1x_2x_5x_6 + x_0x_3x_5x_6. \end{aligned}$$

Using Algorithm 1, with $t = 5$, $c = 11$

$$\{\lambda_0, \lambda_1, \dots, \lambda_7\} = \{\alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6, \alpha^{13}\}$$

are linearly independent elements in D . Then the matrix A in Step 3 of Algorithm 1 is given by

$$\begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

Then, the new basis $\{\beta_0, \beta_1, \dots, \beta_6\}$ is given by

$$(\beta_0, \beta_1, \beta_2, \beta_3, \beta_4, \beta_5, \beta_6) = (1, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6)A^{-1}$$

where

$$A^{-1} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

Hence, we obtain the following new algebraic normal form representation:

$$\begin{aligned} &x_0 + x_5 + x_6 + x_0x_3 + x_1x_3 + x_3x_4 + x_0x_5 + x_1x_6 \\ &+ x_0x_1x_3 + x_0x_2x_3 + x_0x_1x_4 + x_0x_2x_4 \\ &+ x_1x_2x_4 + x_0x_3x_4 + x_2x_3x_4 + x_0x_1x_5 \\ &+ x_0x_2x_5 + x_1x_2x_5 + x_1x_3x_5 + x_2x_3x_5 \\ &+ x_0x_4x_5 + x_0x_1x_6 + x_0x_2x_6 + x_0x_3x_6 \\ &+ x_2x_3x_6 + x_0x_4x_6 + x_1x_4x_6 + x_3x_4x_6 \\ &+ x_1x_5x_6 + x_3x_5x_6 + x_1x_2x_3x_4 + x_0x_1x_3x_5 \\ &+ x_0x_2x_3x_5 + x_0x_1x_4x_5 + x_0x_1x_3x_6. \end{aligned}$$

This Boolean representation of the WG transformation $\text{Tr}(x + x^3 + x^7 + x^{19} + x^{29})$ is a 1-resilient function, and has nonlinearity 56, algebraic degree 4, and linear span 35.

Another example for $n = 11$ can be found in a preliminary version of this work in [9].

VII. CONCLUSION

We provide a table which contains the profiles that we obtained in previous sections as a conclusion of this paper.

In Table I, NC means that there is no corresponding concept.

REFERENCES

- [1] X. Chang, Z. Dai, and G. Gong, "Some cryptographic properties of exponential functions," in *Advances in Cryptology—ASIA CRYPT'94 (Lecture Notes in Computer Science)*. Berlin, Germany: Springer-Verlag, 1994, vol. 917, pp. 415–418.
- [2] J. Dillon, "Multiplicative difference sets via additive characters," *Des., Codes, Cryptogr.*, vol. 17, no. 1–3, pp. 225–235, 1999.
- [3] J. Dillon and H. Dobbertin, "New cyclic difference sets with Springer parameters," preprint, August 1999.
- [4] S. W. Golomb, *Shift Register Sequences*, revised ed. Laguna Hills, CA: Aegean Park, 1982, p. 39.
- [5] G. Gong, P. Gaal, and S. W. Golomb, "A suspected infinity class of cyclic Hadamard difference sets," in *Proc. 1997 IEEE Information Theory Workshop*, Longyearbyen, Svalbard, Norway, July 6–12, 1997.
- [6] R. Gold, "Maximal recursive sequences with 3-valued recursive cross-correlation functions," *IEEE Trans. Inform. Theory*, vol. IT-14, pp. 154–156, Jan. 1968.
- [7] G. Gong and S. W. Golomb, "Transform domain analysis of DES," *IEEE Trans. Inform. Theory*, vol. 45, pp. 2065–2073, Sept. 1999.
- [8] R. Lidl and H. Niederreiter, *Finite Fields*. Reading, MA: Addison-Wesley, 1983, vol. 20, Encyclopedia of Mathematics and its Applications.
- [9] G. Gong and A. M. Youssef, "On Welch–Gong transformation sequence generators," Univ. Waterloo, Waterloo, ON, Canada, Tech. Rep. CORR 2000-30, May 2000.
- [10] J. S. No, S. W. Golomb, G. Gong, H. K. Lee, and P. Gaal, "New binary pseudorandom sequences of period $2^m - 1$ with ideal autocorrelation," *IEEE Trans. Inform. Theory*, vol. 44, pp. 814–817, Mar. 1998.
- [11] A. Maschietti, "Difference sets and hyperovals," *Des., Codes, Cryptogr.*, vol. 14, pp. 89–98, 1998.
- [12] J. M. Massey, "Shift register synthesis and BCH decoding," *IEEE Trans. Inform. Theory*, vol. IT-15, pp. 122–127, Jan. 1969.
- [13] R. J. McEliece, *Finite Fields for Computer Scientists and Engineers*. Boston, MA: Kluwer Academic, 1987.
- [14] J.-S. No, H. Chung, and M.-S. Yin, "Binary pseudorandom sequences of period $2^m - 1$ with ideal autocorrelation generated by the polynomial $z^d + (z + 1)^d$," *IEEE Trans. Inform. Theory*, vol. 44, pp. 1278–1282, May 1998.
- [15] R. A. Rueppel, *Analysis and Design of Stream Ciphers*. Berlin, Germany: Springer-Verlag, 1986, p. 53.
- [16] R. A. Rueppel, "Stream ciphers," in *Contemporary Cryptology: The Science of Information Integrity*, G. J. Simmons, Ed. Piscataway, NJ: IEEE, 1991, pp. 79–80.
- [17] T. Siegenthaler, "Correlation-immunity of nonlinear combining functions for cryptographic applications," *IEEE Trans. Inform. Theory*, vol. IT-30, pp. 776–780, Sept. 1984.
- [18] A. F. Webster and S. E. Tavares, "On the design of S -boxes," in *Advances in Cryptology—Crypto'85 (Lecture Notes in Computer Science)*. Berlin, Germany: Springer-Verlag, 1985, vol. 218, pp. 523–534.
- [19] G. Xiao and J. Massey, "A spectral characterization of correlation immune combining functions," *IEEE Trans. Inform. Theory*, vol. 34, pp. 569–571, May 1988.
- [20] A. M. Youssef and G. Gong, "On the interpolation attacks on block ciphers," in *Proc. Fast Software Encryption 2000 (Lecture Notes in Computer Science)*. New York: Springer-Verlag, 2000, vol. 1978, pp. 109–120.